INFORMATION TECHNOLOGY

Information technology (IT) is an indispensable tool of modern government and one in which the State has invested heavily. However, finding the appropriate governance structure for the State has been challenging. When the statutory authorization for the Department of Information Technology (DOIT) sunset in July 2002, the Administration and Legislature agreed that major reforms were needed to achieve effective statewide planning for and management of information technology.

The Legislature preserved funding in the 2002 Budget Act for two core activities—oversight and security—providing $2 million to the Department of Finance (Finance) for these purposes. The Administration therefore began the 2002-03 fiscal year with three tasks: create an interim IT governance structure during the transition until a new statutory framework could be adopted effective January 1, 2004; implement oversight and security programs that worked; and propose a permanent plan to the Legislature for IT governance.

KEY 2002-03 TASKS

- Create an interim IT governance structure
- Implement oversight and security programs
- Propose a permanent IT governance plan

Information Technology Governance in Transition

In May 2002, the Administration directed state agencies in Executive Order D-57-02 to implement the following IT management reforms:

- **Responsibility and accountability—** Clear assignment of responsibility and accountability for the procurement, management, and operation of the State's information technology systems.
- **Transparency and equity—**Full and fair opportunity for (1) appropriate public input into IT management decisions, and (2) competition among vendors of information technology systems.
- **Ethics—**Clear statement of ethical standards for those individuals who procure, manage, and operate the State's information technology products and services.
- **Informed decisions—**An appropriate needs assessment and fiscal analysis prior to the procurement of new information technology systems.
- **Best value—**Commitment to obtaining quality systems that meet the needs of the State at the best value.

Following the sunset of DOIT in July 2002, the Administration established an interim governance framework, so progress could continue towards these reform goals. Agency secretaries were charged to oversee the management of ongoing information technology and procurement; each department and agency required to develop ethical guidelines for IT; department directors advised to establish direct reporting from chief information officers and chief information security officers; Finance charged with ensuring the continuity and clarity of IT policies, procedures, guidelines, roles, and responsibilities; and the Department of General Services (General Services) charged with ensuring that IT procurement policies and procedures are implemented correctly.

By September 2002, Finance had shut down DOIT's business affairs, formed the new Technology Oversight and Security Unit, streamlined IT policies and procedures (www.dof.ca.gov/HTML/IT/Statewide_IT.htm), reviewed agencies' preliminary oversight reports, and begun planning the new oversight and security programs.

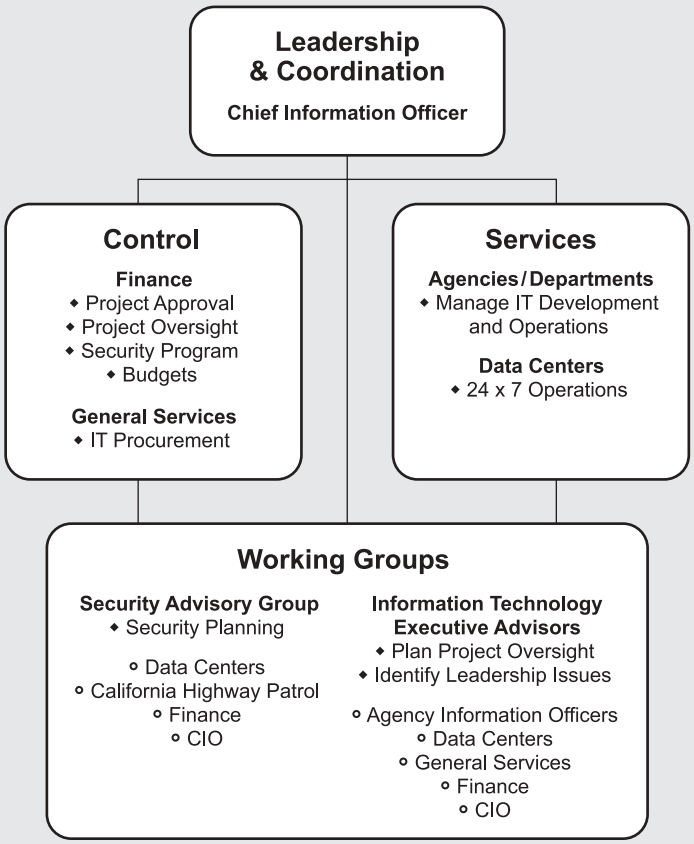
In September, General Services began implementing the procurement reforms recommended in the August 2002 report of the Governor's Task Force on Contracting and Procurement Review (www.dof.ca.gov/html/procurement/final_report.doc). These reforms include enhanced oversight and controls over contracting transactions, a requirement for competition in the California Multiple Award Schedule (CMAS) and Master Agreement programs, development of standards of conduct for state employees as well as contractors involved in contracting transactions, and comprehensive legal participation in all high-risk transactions.

The Administration also appointed a State Chief Information Officer (CIO) within the Governor's Office to coordinate the control agencies and departments that have lead IT responsibilities and to provide leadership on

statewide IT issues. As a result of these efforts, a new approach to IT governance has been created for this transition period—a collaborative model that is neither centralized nor decentralized—with roles and responsibilities defined as follows:

- **Finance** is responsible for project approval and oversight, developing and managing an IT security program, and assisting the State CIO in identifying and addressing key statewide strategic and operational needs for IT management. Finance, with the guidance of the State CIO, is the control agency most directly accountable for ensuring that the fundamentals of IT governance are met during this transition period.
  - **IT executive advisors—**For planning of project oversight and identification of key IT leadership issues, Finance and the State CIO rely on a group of IT executive advisors, made up of the agency information officers, the directors of data centers, and the Department of General Services.
  - **Security advisors—**For security planning, Finance and the State CIO rely on an advisory group made up of the directors for the State's six data centers as well as the California Highway Patrol (CHP). The activities of this group are discussed further below.
- **General Services** is responsible for IT acquisition processes and procedures, including legal counsel. In addition, through its acquisition quality assurance program, General Services is responsible for oversight of all IT procurements conducted by other state agencies. General Services also participates on the IT executive advisors group.
- **Data centers** manage 24-hour, 7 days/week operations for departmental IT systems and are accountable for running a cost-effective, secure business environment. Collectively, the data centers provide services to nearly every state department and therefore are

INTERIM STRUCTURE FOR IT



assigned a leadership role as members of both the executive and security advisory groups.

- **Each department** is responsible for effectively managing its information technology development and operations, including providing ethical guidelines for IT procurements; creating direct lines of reporting between directors and the department's CIO and information security officer; providing independent oversight of projects; and implementing basic security measures.
- **Each cabinet-level agency** provides leadership, coordination, and oversight of IT activities and procurements within its jurisdiction. Agencies have assumed a larger role during this transitional period of IT governance for oversight of projects and advising Finance and the State CIO on IT leadership issues.
- **The CHP** has a key role in IT security, handling security incident notification and criminal investigation, and as a member of the advisory group.

During this transition, the State CIO is working with the State's primary IT executives to safeguard IT infrastructure and projects and to address immediate priorities and planning needs. This is a leadership and consultative role, without direct operational or project responsibilities. Instead, the agencies and departments that are statutorily responsible and accountable for state operations are working together, under the State CIO's guidance, to meet IT governance needs.

Implementing Successful Project Oversight

Common problems encountered in delivering projects are incomplete scope definitions or cost estimates, projects that exceed the skill level or organizational capacity of a department, evolving business and technology requirements, and changing statutory or federal requirements. While departments have the primary responsibility for effective oversight of a project, outside assistance is often necessary, depending on the risk involved.

Under the former governance structure for IT, DOIT provided oversight assistance for department's IT projects. Following the sunset of DOIT, the Administration in Executive Order D-59-02 directed departments and agencies to assume full responsibility for oversight and report steps taken to Finance. Subsequently, the 2002 Budget Act appropriated funds to Finance to implement a statewide oversight program.

Finance has defined project oversight, assigned broad roles building on the direction provided in the Executive Order, and is currently developing a framework for project reviews and reporting. Finance defines project oversight as an independent review and analysis of specific project activities and documentation to determine if the project is on track to be completed within the estimated schedule and cost, and will provide the functionality required by the sponsoring business entity. Project oversight identifies and quantifies any issues and risks affecting

these project components and implements appropriate remediation plans for the identified project risks.

Finance will categorize IT projects by their risk, sensitivity and/or criticality, and also assess the department's overall ability to deliver projects, to determine whether a project will be monitored by the department alone, by the department and agency, or by the department, agency, and Finance. Finance will oversee the State's most critical IT projects and also assist as necessary in remediation planning for projects overseen at the agency level. Finance will keep the Administration and the Legislature informed of project oversight activities, project risks, and remediation efforts. And finally, because project management and oversight skills and organizational structure are strong factors in project success, Finance will evaluate the IT practices of departments and agencies.

By February 1, 2003, Finance will publish its detailed criteria for project oversight; the criteria for assessing department and agency project management and oversight practices; project lists that identify, for each project, the oversight level; initial project oversight reporting forms and guidelines; and reporting schedules.

Securing Information Technology Assets and Information

In the aftermath of September 11, and in the wake of the intrusion into Teale Data Center in 2002, IT security is an even more important concern for State government.

The Legislature provided funding for Finance to develop a security program in 2002-03. Finance reached out to key partner agencies for planning assistance, creating an interagency "community" approach to a security program. This approach relies on clear definition of roles and wise use of the existing resources to create an informed community of state IT professionals who focus on mitigating the highest IT security risks.

Key players in IT security include:

- **Finance,** in consultation with the State CIO, has overall responsibility for the policy and procedural framework for the program. Finance disseminates security information to departments and agencies; reviews departments' annual operational recovery plans; works through the security advisory group to support departments during security incidents; receives and follows up on written incident reports for security incidents referred by the CHP; develops security assessment and audit criteria; and provides educational and awareness information.
- **The Security Advisory Group** provides practical guidance to Finance and the State CIO in the management of the statewide IT security program. Members are: the directors of the Stephen P. Teale Data Center, Health and Human Services Agency Data Center, Hawkins Data Center Bureau, Franchise Tax Board's Computing Resources Bureau, the Legislative Data Center, and CalPERS' Data Center; and the CHP. The advisory group helps to identify

high priority IT security activities based on risk and available resources, and how to complete them.

- **The CHP** is responsible for law enforcement related to criminal IT security intrusions, operates the State's incident notification center, and participates in the security advisory group. Currently, state departments are required to contact both Finance and the CHP when an IT security intrusion occurs. By February 1, 2003, these contact points will be consolidated and the CHP will receive all security incident notifications, passing non-criminal matters on to Finance. The CHP also conducts criminal investigations when security incidents occur that warrant this action.
- The various departmental **Information Security Officers** (ISOs) are risk managers who oversee the implementation of security practices for their departments and monitor and report security incidents.

Department CIOs also play a key role in the statewide security program, managing the technology that supports statewide security efforts as well as departments' IT programs. In most cases, the technical employees who perform the hands-on security work report to the CIOs. In addition, Agency Information Officers (AIOs) establish agency-wide security programs and protocols, as appropriate.

Critical next steps for IT security—Using current assets wisely is particularly important in this fiscal environment. Existing IT security resources need to be identified, they need to communicate well with each other, and Finance needs to help departments focus on high risks and respond effectively to security incidents. IT security is a community concern: information sharing throughout government, although valuable and necessary, means that a weak link can have broad repercussions. Initial tasks include:

- **Identifying existing statewide security resources and authorities—**By mid-April 2003, Finance will identify statutory authorities, State Administrative Manual policies, and resources in place to support statewide and departmental security activities.
- **Implementing a security communication plan—**During the first half of calendar year 2003, Finance will phase in a statewide security communication plan.
- **Beginning risk identification—**There is much to do in identifying and mitigating risks. During the first quarter of calendar year 2003, Finance will work with the Security Advisory Group to identify relatively low-cost steps to mitigate serious risks, then survey departments to assess whether these security measures and practices have been implemented. Finance will then work with the security advisory group to identify and implement follow-up measures.
- **Improving security awareness and knowledge—**Starting in the first quarter of 2003, there will be a periodic security forum for department ISOs. Finance

will also establish a web site to share security awareness information and advice.

- **Managing security incidents—**Processes for security incident notification and follow-up reporting are being updated. By February 1, 2003, Finance will publish the updated process that incorporates new protocols.
- **Ensuring the confidentiality of security information—**The Administration is proposing legislation to ensure that information on the State's IT security operations is afforded an appropriate level of confidentiality.

THE SECURITY COMMUNITY

- State CIO
- Finance
- The Security Advisory Group
- CHP
- Department Information Security Officers
- CIOs and Agency Information Officers

Towards a New Statutory Framework for Information Technology Governance

The first step towards a permanent governance structure is to build consensus on a broad vision for the use of information technology in state operations and on basic governance principles that guide the State towards that vision. For now, the CIO has operated pursuant to the following working vision: *The State will manage, deploy, and develop its information technology resources to support responsive and cost-effective state operations, and to establish timely and convenient delivery of state services, benefits, and information.* However, this vision will evolve as discussions unfold with the Legislature.

Designing a statutory framework should also involve a discussion of underlying principles. The Administration believes that effective statewide management of information technology is based on clear strategic thinking, sound management of the existing IT operations, and demonstrated accountability. The future governance structure for IT needs to address all three requirements. In particular, public trust in the State's IT governance needs to be restored.

The Administration believes that a new IT governance structure must be aligned with and responsive to the complex, decentralized structure of California government. In both strategic decision-making and operational implementation, effective coordination across organizational boundaries is itself a primary strategic objective.

KEY PRINCIPLES FOR IT GOVERNANCE

1. Cost-effective IT driven by business needs and procured through a competitive process.
2. CIO as the system architect and planner.
3. Statewide strategies based upon broad input.
4. Planning for present and future.
5. A forum to coordinate IT governance.
6. A bridge between strategic decision making and operational accountability.
7. Assignment of governance tasks based on expertise.
8. Transparency and opportunity for public input.
9. Clearly assigned roles and responsibilities.
10. A strong policy and procedural framework that is enforced.
11. Departments, agencies, control agencies all enforce compliance.
12. IT performance and progress is assessed and reported.

The Administration has previously suggested, and continues to believe, that an Information Technology Board could serve effectively in providing both leadership and coordination. While there are many important issues to be resolved in how the Board would operate, the Administration offers the following organizational principles as guidance:

For successful strategic thinking:

- Cost-effective IT must be driven by the State's business and program needs—not by the technology itself—and procured through a competitive process.
- The CIO should be the system architect and planner, not the contractor or the plant manager. Organizationally, strategic planning should be separate from but informed by day-to-day operational activities.
- Statewide strategies should be based upon broad input, drawing upon the knowledge, vision, and most effective practices of successful public, private, and educational organizations.
- Planning must have relevance for both current and anticipated needs.

For sound administration of operations:

- A forum, such as the Board could provide, is needed to coordinate main providers of IT governance (the CIO as strategic thinker, the control agencies that provide program structure and accountability, the data centers, and departments that manage operations).
- There must be a bridge between strategic decision-making and operational activity. The Board could provide that bridge.
- Sound administration is based on assigning governance tasks by expertise: service agencies primarily have

operational responsibility, control agencies have oversight responsibilities, the CIO should remain primarily at the strategic level, and the Information Technology Board could provide a public forum for coordination and the highest level of program oversight.

To ensure accountability:

- There must be transparency and an opportunity for public input to strategic decision-making and major operational implementations.
- Roles and responsibilities must be clearly assigned.
- The policy and procedural framework for IT management must be clear, consistent, updated, and enforced.
- The responsibility for ensuring compliance with state policy and procedure must be embraced at each level of governance: project managers, department ISOs, department CIOs, department directors, agency secretaries, General Services, Finance, and the State CIO. Each must be accountable for prompt, effective action.
- IT performance and progress, at both the project and department level, must be assessed and reported to ensure the effective management and control of IT activities and the enforcement of State policies and procedures.

By February 1, 2003, the Administration will provide a specific proposal and draft legislation for a permanent IT governance structure that is based on the principles above.

The State's Fiscal Challenge and Information Technology

In light of the State's fiscal constraints, it must meet two IT leadership objectives. The first is to identify key IT investments and ensured they are preserved. The second is to take advantage of downsizing by using IT as a transformational tool to assist programs in maintaining services through IT strategies, where practicable.

Assessing impacts on IT investments— The IT management objective during downsizing is to identify departments' key IT investments and to develop strategies to keep them functioning. IT challenges may arise from reduction, elimination, consolidation, or realignment of program services as well as from staffing reductions. Finance will work with agencies and departments to assess impacts on key IT investments and will report initial findings by the May Revision.

Using IT as a downsizing strategy—For some programs, IT can also help mitigate the effect of budget reductions by providing alternative, less costly methods of service delivery. For example:

- The Department of Conservation will reduce the traditional public outreach and library services within the Geologi-

cal Survey Library. Currently, the Library provides various geological books, maps, and publications. In order to use these documents, members of the public have to contact Conservation, and in some cases, travel to Sacramento from other locations. Conservation can save $600,000 by placing these publications online, and at the same time improving public access.

- The California Environmental Protection Agency will close its two Permit Assistance Centers, relying on the CalGOLD website to provide permit and license information online, for a savings of $85,000 in 2002-03 and $339,000 in 2003-04.
- The Franchise Tax Board (FTB) will require the mandatory electronic filing of returns for tax practitioners filing 100 or more returns. FTB estimates that mandatory electronic filing would result in an additional 2.5 million to 4 million electronically filed returns annually, for a savings of $1.49 million in 2003-04.

Using IT to be more responsive to the public and businesses—Some programs use IT as a means to provide alternative access to services and information for the public and businesses. For example:

- **Department of Consumer Affairs Professional Licensing—**Through 36 professional boards and bureaus, consumers can look up licensure information online about professionals or companies that provide services. Also, seven professions, including barbers and cosmetologists, dentists, physicians, and registered nurses, can register or renew professional licenses online. These Internet-based services open the doors of state government 24 hours a day, 7 days a week.
- **Department of Pesticide Regulation (DPR) Online Access to Pesticide Use, Registration, and License Information—**The DPR created an online system that allows the public to confirm that pest control businesses and applicators have the required licenses. In addition, a pilot project allows licensees to annually register with counties online, rather than having to visit each county where they wish to do business. The DPR also created a new database application that posts licensing exam scores online within minutes, rather than requiring days before written notification to applicants. The DPR revamped and posted data online in searchable formats that made it more immediately accessible to the public. This information includes pesticide use reports, pesticide illness reports, and a massive surface water database. In January 2003, the DPR will launch the "California Pesticide Information Portal" to allow the public to generate customized summaries of pesticide use data by county, crop, and year. Also in 2003, the DPR will launch a program to automatically give registrants e-mail updates on the status of pending pesticide registrations.
- **Department of Toxic Substances Control Web-based Hazardous Waste Tracking Information—**In June 2002, the Department activated its new Hazardous Waste Tracking System that

will eventually replace the six-part paper form used to track hazardous waste from cradle to grave. At present, generators can track their waste streams, confirm invoicing, and look-up their federal EPA Identification numbers. Transporters can confirm that the generators from whom they are picking up waste have valid identification numbers. And, the web-based system enables public interest and environmental groups to research all manner-of-facts and trends relating to hazardous waste generation, transportation, and disposal.

- **Department of Motor Vehicles (DMV) Online Vehicle Registration and Driver License Appointments—**DMV customers can now make appointments for vehicle registration and driver license appointments online. An online application allows customers to renew their vehicle registrations over the Internet. Electronic evidence of insurance is now available to verify the insurance status of a vehicle without burdening the vehicle owner, and enabling registration by phone and Internet.

- **California Film Commission (CFC) Comprehensive Website—**The entertainment industry employs more than 300,000 people per year and generates more than $32.3 billion in California. On November 5, 2001, the CFC unveiled its new revamped website (www.film.ca.gov). This website allows producers, directors, and location scouts an opportunity to download pertinent paperwork, information, and contact information in an effort to sustain California's position as the undisputed leader in the global entertainment industry. In addition, this website provides access to a fully interactive web-based program called CinemaScout. CinemaScout allows location scouts to view and to preview various potential filming sites up and down the State.

- **Employment Development Department (EDD) Job Service—**CalJOBS, EDD's electronic job match system, is continuously upgraded to add new functionality and make the system easier to access for users. Major enhancements planned in the near future include installation of a Job Scout and e-mail feature to allow the system to automatically alert job seekers by e-mail if a job is entered that meets job criteria they have specified. Additionally, CalJOBS is piloting language translation software to allow Spanish speaking job seekers to view information in the system in Spanish. Finally, CalJOBS is being updated to parallel the appearance of the Governor's Homepage and other California Government Internet sites. This effort will increase the familiarity of users and employ the same general navigation as other Government sites, making the system more user friendly.

- **Franchise Tax Board (FTB) California Tax Information Center—**The California Tax Information Center at www.taxes.ca.gov offers one-stop federal and California tax information and assistance for business owners. This site is sponsored by the California FedState Partnership (EDD, FTB, BOE, and IRS) to provide streamlined access

to tax information. For small businesses, the site contains the *Striking Gold in California* booklet with tax information, a tax calendar with due dates for reports and payments, and the Small Business Assistance Center with links to other sites of interest for small business owners.

- **Teacher Credentialing Service Improvement Program—**The Commission on Teacher Credentialing (CTC) created an online system to allow teachers to apply for renewals of their credentials and allow the public to verify the status of a teacher's credential. The CTC currently is working on the final phase of this project, which will allow teachers to apply for an initial credential online. This final component of the system is expected to be completed in July 2003.

As departments continue to evaluate the impact of budget reductions on their operations, the Administration expects them to identify further opportunities to use information technology to meet the challenge.